

Amendments to the Claims:

A listing of the entire set of pending claims (including amendments to the claims, if any) is submitted herewith per 37 CFR 1.121. This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A system comprising an information carrier for comprising user-information and an apparatus for accessing the information carrier, the information carrier comprising an optical identifier representing a physical one-way function and authentication information, the apparatus comprising:

a light source for providing a set of challenges to the optical identifier in a single authentication phase giving rise to a corresponding set of responses, when the information carrier is present in the apparatus, the set of challenges [[challenge]] being generated by a light beam incident on the optical identifier,

a computational unit for applying a mathematical function to the corresponding set of responses,

a detector for detecting the corresponding set of responses to the set of challenges as different speckle patterns produced by the optical identifier upon being challenged with the light beam,

a reading unit for reading the authentication information,

a verification unit for comparing the corresponding set of responses with the authentication information, the authentication information being related to the response.

applying the first one-way function to the each challenge to obtain a first result,

applying the second one-way function to the corresponding response to obtain a second result,

2. (Previously Presented) A system as claimed in claim 1 wherein the user-information present in the information carrier is encrypted, and in the apparatus:

the reading unit (18) is further capable of reading the user-information,

a decryption key extraction unit is present, for extracting a decryption key from the response, and

a decryption unit is present, for decrypting the user-information encrypted with the decryption key.

3. (Cancelled)

4. (Previously Presented) A system as claimed in claim 1, wherein the apparatus is able to select a subset of challenges from the set of challenges, to challenge the optical identifier with challenges belonging to the subset of challenges, and to detect a subset of corresponding responses.

5. (Previously Presented) A system as claimed in claim 1, wherein the authentication information is further related to the set of challenges.

6. (Previously Presented) A system as claimed in claim 5, wherein the authentication information is in the form of a table having a record for each challenge belonging to the set of different challenges, the record having in a first field the result of a first one-way function applied to the each challenge, and in a second field the result of a second one-way function applied to the corresponding response.

7. (Currently Amended) A system as claimed in claim 6, wherein the verification unit is able to execute, for the each challenge, the following steps:

applying the first one-way function to the each challenge to obtain a first result,

applying the second one-way function to the corresponding response to obtain a second result,

identifying a record in the table having in the first field a value equal to the fist result, and

[[[-]] reading from the record identified the value present in the second field (33), and comparing it with the second result.

8. (Previously Presented) A system as claimed in claim 1, wherein the apparatus comprises means for monitoring a time elapsing between challenging the optical identifier and detecting the speckle pattern.

9. (Currently Amended) An information carrier for comprising user-information, the information carrier comprising an optical identifier representing a physical one-way function which is able to produce a set of speckle patterns as a set of responses upon being challenged with a modulated light beam as a set of challenges, and further comprising authentication information related to the set of responses, the authentication information comprising the result of a mathematical function applied to the set of responses.

10. (Previously Presented) An information carrier as claimed in claim 9, wherein the user-information is encrypted and is decryptable with a decryption key extractable from the response.

11. (Previously Presented) An apparatus for accessing an information carrier for comprising user-information, which information carrier comprises an optical identifier representing a physical one-way function and authentication information, comprising:

a light source for providing a set of challenges to the optical identifier in a single authentication session giving rise to a corresponding set of responses, when the information carrier is present in the apparatus, the challenge being generated by a light beam incident on the optical identifier,

a detector for detecting the corresponding set of responses to the set of challenges as different speckle patterns produced by the optical identifier upon being challenged with the light beam,

a computational unit for applying a mathematical function to the corresponding set of responses,

a reading unit for reading the authentication information, and

a verification unit for comparing the corresponding set of responses with the authentication information, the authentication information being related to the response.

12. (Currently Amended) A method for accessing an information carrier comprising user-information, which information carrier comprises an optical identifier representing a physical one-way function and authentication information, comprising:

a challenging step, for challenging the optical identifier with a set of challenges via a light beam modulated to provide the set of challenges,

a detecting step, for detecting a set of speckle patterns produced by the optical identifier as a set of responses [[response]] upon being challenged with the set of challenges via the modulated light beam,

a reading step, for reading the authentication information from the information carrier, [[and]]

a computational step for applying a mathematical function to the set of responses, and

a verification step, for comparing the set of responses [[responses]] produced by the optical identifier upon being challenged with the set of challenges via the modulated light beam and the authentication information read from the information carrier, the authentication information being related to the response produced by the optical identifier.

13. (Currently Amended) A computer readable medium having computer readable instructions embedded therein which instructions when executed by the computer causing a processor to execute a method for accessing an information carrier comprising user-information, which information carrier comprises an optical identifier representing a physical one-way function and authentication information, comprising:

a challenging step, for challenging the optical identifier with a set of challenges via a light beam modulated to provide the set of challenges,

a detecting step, for detecting a set of speckle patterns produced by the optical identifier as a set of responses [[response]] upon being challenged with the set of challenges via the modulated light beam,

a reading step, for reading the authentication information from the information carrier, and

a computational step for applying a mathematical function to the set of responses, and

a verification step, for comparing the set of responses [[responses]] produced by the optical identifier upon being challenged with the set of challenges via the modulated light beam and the authentication information read from the information carrier, the authentication information being related to the response produced by the optical identifier.